Configuring Service EPGs Using Nexus Dashboard Orchestrator

Revised: February 19, 2022,

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior

Feature or Change	Description	Where Documented
Initial release of document	Initial release of document.	

About Cloud Service Endpoint Groups

Note The following content refers to "Multi-Site Orchestrator" which has been rebranded to Nexus Dashboard Orchestrator. Same information is applicable to both products.

A cloud service EPG is a managed object that is a named logical entity that contains a collection of cloud native or third-party service instances or endpoints. In this situation, an endpoint refers to a particular service instance. For example, an SQL server would be considered an endpoint, and a collection of SQL servers would form a service endpoint group. Other examples of service EPGs would be a collection of Storage Accounts, a collection of Key Vaults, and so on.

Service EPGs have several unique attributes:

- Service Type: This attribute indicates what type of cloud service is being grouped. Examples of available service types include Azure SQL, Azure Containter Registery, Azure ApiManagement Services, and so on. The service type Custom is used when configuring a third-party service EPG.
- Deployment Type: This attribute indicates how and where the service is deployed. Following are the available deployment types:
    - Cloud Native: In this type of deployment, the service is instantiated in the cloud provider's network and the user or applications consuming it have a handle to the service. For example, an Azure storage account might reside inside Azure's own VNet, and you would have a URL to access the storage contents.
    - Cloud Native Managed: In this type of deployment, the service is instantiated in your VNet or subnet (created through the Cisco Cloud APIC). For example, an Azure Kubernetes cluster (AKS) could be deployed in a subnet that is managed by the Cisco Cloud APIC.
    - Third-Party: This is a deployment where a third-party (not Azure) is providing services through the market place. Access to this service is provided through the private links feature.
- Access Type: This indicates how the service will be accessed. Following are the available access types:
    - Public: The service will be accessed using the public IP address assigned to it. Access to the public IP address range of a particular service is achieved using the Azure "Service Tags" in the NSG rules.
    - Private: The service will be accessed using a private IP address assigned to it. This assignment is done through the creation of private endpoints when the deployment is of type Cloud Native. In the case of a Cloud Native Managed deployment, the private IP is assigned by the service from the subnet IP space.

Only certain deployment types, and certain access types within each deployment type, are supported for each service type, described in the previous bullets. The following table provides more information on the deployment types and access types that are supported for each service type.

Service Type	Provider	Deployment Type/Access Type		
		Cloud Native	Cloud Native Managed	Third-Party
Azure Storage Blob	Microsoft.Storage	Private	N/A	N/A
Azure SQL	Microsoft.Sql	• Public • Private	N/A	N/A
Azure Cosmos DB	Microsoft.DocumentDB	• Public • Private	N/A	N/A
Azure Databricks	Microsoft.Databricks	Public	• Private • Public and Private	N/A
Azure Storage	Microsoft.Storage	• Public • Private	N/A	N/A
Azure Storage File	Microsoft.Storage	Private	N/A	N/A
Azure Storage Queue	Microsoft.Storage	Private	N/A	N/A
Azure Storage Table	Microsoft.Storage	Private	N/A	N/A
Azure Kubernetes Services (AKS)	Microsoft.ContainerService	Private	• Private • Public and Private	N/A
Azure Active Directory Domain Services	Microsoft.AAD	Public	• Private • Public and Private	N/A
Azure Container Registry	Microsoft.ContainerRegistry	• Public • Private	N/A	N/A
Azure ApiManagement Services	Microsoft.ApiManagement	Public	• Private • Public and Private	N/A
Azure Key Vault	Microsoft.KeyVault	• Public • Private	N/A	N/A

Service Type	Provider	Deployment Type/Access Type		
		Cloud Native	Cloud Native Managed	Third-Party
Redis Cache	Microsoft.Cache	N/A	• Private • Public and Private	N/A
Custom Service		• Public • Private	N/A	Private

- Service Endpoint selectors: Service endpoints can be selected using the existing selectors (used in the cloud EPG selection) as well as the new types of selectors listed below:
  - Resource Name: The service resource's name
  - Resource ID: The cloud provider's ID for the resource
  - URL: The alias or FQDN that identifies the service (the private link alias is used in Azure)

  The following table provides more information on the endpoint selectors that are supported for each deployment type.

Note Information for the Cloud Native (Public) deployment type is not provided in the following table because that deployment type does not support endpoint selectors.

Deployment Type	Tags	Region	IP	Resource Name	Resource ID	URL
Cloud Native (Private)	Y	Y	N	Y	Y	N
Cloud Native Managed	N	N	Y	N	N	N
Third-Party	N	N	N	N	N	Y (applicable only for private link connection)

Guidelines and Restrictions for Cloud Service EPGs

- You must have the NSG-per-subnet configuration enabled if you are configuring cloud service EPGs.
- A service EPG with a Cloud Native deployment type and a Public access type requires an NSG rule to allow access to the Azure PaaS service using Azure-defined tags. Cisco ACI Multi-Site Orchestrator will create the NSG rule only on sites where the service EPG that is configured as Cloud Native/Public is present; ACI Multi-Site Orchestrator will not create the NSG rule for remote sites. To make this work, local deployment of that service EPG should be present on all the sites.

  For example, assume ACI Multi-Site Orchestrator is managing two sites (site1 and site2):
  - Site1 contains the service EPG configured as Cloud Native/Public, so ACI Multi-Site Orchestrator creates the NSG rule to allow access to an Azure PaaS service using the Azure-defined tags (for example, the Azure Key Vault service). Site1 is the provider for this service.

- Site2 is the consumer for this service, and wants to access to site1's Azure Key Vault service.

In this situation, ACI Multi-Site Orchestrator will program the site1 VMs, but will not program the site2 VMs, so the site2 VMs cannot access the Azure Key Vault service provided by site1.

To make this work, deploy the Azure Key Vault service in site2 as well, where that Azure Key Vault service is just a dummy service, with no resources. By enabling that Azure Key Vault service on site2, the site2 VMs can then access the Azure Key Vault service on site 1 through ACI Multi-Site Orchestrator.

About Service Types

Additional information specific to certain service types are provided below:

- Azure Storage, on page 5
- Azure ApiManagement Services, on page 6
- Azure Databricks Services, on page 6
- Azure Active Directory Domain Services, on page 6
- Azure Kubernetes Services, on page 6
- Azure Redis Cache, on page 7

Azure Storage

The Azure Storage service type is a general service type that can be broken down into four subtypes:

- `Blob`
- `File`
- `Table`
- `Queue`

If you were to configure a service EPG with the following values, using the general Azure Storage service type:

- Service type: `Azure Storage`
- Deployment type: `Cloud Native`
- Access type: `Private`

Then four private endpoints are automatically configured for this service EPG, one for each of the four subtypes listed above.

However, if you were to configure a service EPG with the following values, using a more specific Azure Storage service type:

- Service type: One of these service types:
  - `Azure Storage Blob`
  - `Azure Storage File`
  - `Azure Storage Table`
  - `Azure Storage Queue`

- Deployment type: `Cloud Native`
- Access type: `Private`

Then only one private endpoint is automatically configured for this particular subtype for this service EPG.

Note that the four specific Azure Storage subtypes (`Blob`, `File`, `Table`, and `Queue`) are not allowed if you have an access type of `Public` with the deployment type of `Cloud Native`. This is because Azure service tags are not storage subtype specific.

Azure ApiManagement Services

For an Azure ApiManagement (APIM) Services instance to be deployed in a VNet, it needs to be able to access a lot of other Azure services. In order to do this, the security group rules that allow this access must be programmed.

Cisco Cloud APIC automates this and configures the rules listed here:

https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet#-common-network-configuration-issues

Azure Databricks Services

Azure Databricks requires the following:

- Access to other services
- Two subnets for deployment, where the subnets are delegated to Microsoft

For Azure Databricks, make the following configurations:

- Before configuring the service EPG, you must configure two subnets specifically for the Azure Databricks Services.
- When configuring the service EPG, you must create two service endpoint selectors that will be used to match the two service subnets.

Once the subnet is identified with the Azure Databricks service EPG through the configured endpoint selectors, Cisco Cloud APIC delegates subnets to Azure and configures the rules listed here:

https://docs.microsoft.com/en-us/azure/databricks/administration-guide/cloud-configurations/azure/vnet-inject

Azure Active Directory Domain Services

Azure Active Directory Domain Services (ADDS) requires the following:

- Access to other services
- No routing table is attached to the subnet when it is being deployed

The action of de-associating the routing table from the subnet should be done through the Azure portal after configuring the service EPG and before deploying ADDS. The routing table can be attached to the subnet after the deployment is completed.

Cisco Cloud APIC automates the programming of the rules listed here:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/network-considerations

Azure Kubernetes Services

Azure Kubernetes Services (AKS) requires access to other services.

Cisco Cloud APIC automates the programming of the rules listed here:

https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic#required-outbound-network-rules-and-fqdns-for-aks-clusters

Azure Redis Cache

Azure Redis cache requires access to other services.

Cisco Cloud APIC automates the programming of the rules listed here:

https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-how-to-premium-vnet#outbound-port-requirements

About Deployment Types

Additional information specific to certain deployment types are provided below:

- Cloud Native, on page 7
- Cloud Native Managed, on page 8

Cloud Native

In this type of deployment, the service is instantiated in the cloud provider's network and the user or applications consuming it have a handle to the service. For example, an Azure storage account might reside inside Azure's own VNet, and you would have a URL to access the storage contents.

The following is an example service EPG with a Cloud Native deployment type:

- Service Type: Azure SQL
- Deployment type: Cloud Native
- Access type: Private

In this example scenario, you would make the following configurations in this order:

1. In the Cisco ACI Multi-Site Orchestrator, create a private link label in a cloud context profile to be used by the Azure SQL service EPG.

   Follow the procedures in Tasks To Perform Prior to Configuring Service EPGs, on page 9. Configure a private link label to be used by the Azure SQL service EPG (for example, `SQL-PLL`).

2. In the Cisco ACI Multi-Site Orchestrator, create a service EPG of the service type Azure SQL.

   Follow the procedures in Creating a Service EPG, on page 9, using the following parameters:

   - Service Type: Azure SQL
   - Deployment type: Cloud Native
   - Access type: Private

   When you are configuring the endpoint selector as part of the process of configuring this type of service EPG, configure the endpoint selector to match the appropriate value for the SQL server.

   For example, if you wanted to select an SQL server with the name `ProdSqlServer`, you would make the following selections:

   - Key: Name
   - Operator: equals
   - Value: `ProdSqlServer`

As another example, if you wanted to select an SQL server using the cloud provider's resource ID of `/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer`, you would make the following selections:

- Key: Resource ID
- Operator: equals
- Value: `/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer`

3. In the Azure portal, configure the Azure SQL resources in the cloud.

Cloud Native Managed

In this type of deployment, the service is instantiated in your VNet or subnet (created through the Cisco ACI Multi-Site Orchestrator). For example, an Azure ApiManagement Services could be deployed in a subnet that is managed by the Cisco ACI Multi-Site Orchestrator.

The following is an example service EPG with a Cloud Native Managed deployment type:

- Service Type: Azure ApiManagement Services
- Deployment type: Cloud Native Managed
- Access type: Private

In this example scenario, you would make the following configurations in this order:

1. In the Cisco ACI Multi-Site Orchestrator, create a subnet in a cloud context profile to be used by the Azure ApiManagement Services service EPG.

   Follow the procedures in Tasks To Perform Prior to Configuring Service EPGs, on page 9. Configure a subnet to be used by the Azure ApiManagement Services service EPG (for example, `10.50.0.0/16`).

2. In the Cisco ACI Multi-Site Orchestrator, create a service EPG of the service type Azure ApiManagement Services.

   Follow the procedures in Creating a Service EPG, on page 9, using the following parameters:

   - Service Type: Azure ApiManagement Services
   - Deployment type: Cloud Native Managed
   - Access type: Private

   When you are configuring the endpoint selector as part of the process of configuring this type of service EPG, configure the endpoint selector to match the IP address that you used when you created a subnet in the cloud context profile in the first step.

   For example, using the example provided in the first step, you would configure this endpoint selector for this service EPG:

   - Key: IP
   - Operator: equals
   - Value: 10.50.0.0/16

3. In the Azure portal, configure the Azure ApiManagement Services resources in the cloud.

Tasks To Perform Prior to Configuring Service EPGs

Before you can configure a service EPG, there are certain tasks that you might have to perform beforehand. If you are using subnets or private link labels with your service EPG, you must first configure the subnets and/or private link label on the site local.

Procedure

Step 1 In the middle pane in the page, scroll down to VRFs and select an existing VRF or create a new one.

Step 2 In the right pane in the page, click Add Region.

The Add Cloud Region CIDRs window appears.

Step 3 Make the following selections:

- Region: Select the region.
- Context Profile Type: Select the context profile type.
- CIDR: Click Add CIDR, then add the CIDR.
- CIDR Type: Select Primary or Secondary.
- Select Associated VRF: Select Parent VRF or Hosted VRF.
- In the Add Subnets area:
  - Subnet: Enter the subnet for the CIDR.
  - Name: Enter a name for the subnets.
  - Private Link Label: Enter a name for the private link label.

Step 4 Click Save.

Creating a Service EPG

This section explains how to create a service EPG through the Cisco ACI Multi-Site Orchestrator GUI. Each service needs at least one consumer EPG and one provider EPG.

Before you begin

- Review the information in About Cloud Service Endpoint Groups, on page 2.

  You will be selecting the deployment type and service type in these procedures, but only certain deployment types are supported for each service type. See About Cloud Service Endpoint Groups, on page 2 for more information on the deployment types that are supported for each service type.

- Verify that you have the NSG-per-subnet configuration enabled.

Procedure

Step 1 In ACI Multi-Site Orchestrator, navigate to Application Management > Schemas.

The Schemas window appears.

Step 2 Create a new schema or edit an existing one.

Step 3 In the overview page for that schema, create a new template or edit an existing one.

Step 4 Click the … (3 dots) on the template that you want to edit and click Add Sites.

Step 5 Add the necessary sites to the template and click Save.

You're returned to the templates page.

Step 6 Scroll down to EPGs and click Add EPG.

Step 7 Enter the appropriate values in each field as listed in the following Create EPG Dialog table then continue.

Table 2: Create EPG Dialog

Properties	Description
General	
Display Name	Enter the name of the EPG.
Contract	Add a new contract.
EPG Type	Choose Service.
Virtual Routing and Forwarding	Select an existing VRF or create a new VRF.
Deployment Type	Choose the EPG deployment type. Services are differentiated based on their deployment mode: • Cloud Native: A Cloud Native service deployed in the provider network • Cloud Native Managed: A Cloud Native service deployed in your network • Third-Party: A third-party service from the market place

Properties	Description

Access Type	Choose the EPG deployment access type. The choices vary, depending on the selection you made in the Deployment Type field:
	• Cloud Native deployment type:
	  • Public: Access the public IP of the service.
	  • Private: Use private links and private endpoints to access the service.
	• Cloud Native Managed deployment type:
	  • Private: Choose this type if the service deployed in the managed subnet has only private IP addresses.
	  • Public and Private: Use public and private endpoints to access the service. This is used for services that also expose public IP addresses when deployed in Cisco Cloud APIC-managed subnets.
	• Third-Party deployment type: Private is the only option available to you as an access type. This means that you will use only private endpoints to the service, if the service offers it.

Service Type	Choose the Azure service type. The options are: • Azure Storage Blob (see Azure Storage, on page 5) • Azure SQL • Azure Cosmos DB • Azure Databricks (see Azure Databricks Services, on page 6) • Azure Storage (see Azure Storage, on page 5) • Azure Storage File (see Azure Storage, on page 5) • Azure Storage Queue (see Azure Storage, on page 5) • Azure Storage Table • Azure Kubernetes Services (AKS) (see Azure Kubernetes Services, on page 6) • Azure Active Directory Domain Services (see Azure Active Directory Domain Services, on page 6) • Azure Container Registry • Azure ApiManagement Services (see Azure ApiManagement Services, on page 6) • Azure Key Vault • Redis Cache (see Azure Redis Cache, on page 7) • Custom Service (used if you choose Third-Party as the Deployment Type below)

Step 8 Complete the remaining fields to finish creating the service EPG, depending on the selection you made in the Deployment Type field:

- If you chose Cloud Native as the deployment type, go to Configuring Cloud Native as the Deployment Type, on page 12.
- If you chose Cloud Native Managed as the deployment type, go to Configuring Cloud Native Managed as the Deployment Type, on page 14.
- If you chose Third-Party as the deployment type, go to Configuring Third-Party as the Deployment Type, on page 16.

Configuring Cloud Native as the Deployment Type

Use the procedures in this section to configure Cloud Native as the deployment type for the service EPG.

Procedure

Step 1 Navigate to site local.

Step 2 In the middle pane, scroll down to EPGs and click the service EPG that you just created.

Step 3 In the right pane, scroll down to the Selectors area.

Step 4 If you selected Private as the access type, the Private Link Labels option becomes available.

A private link label is used to associate the subnets to the service EPGs.

Step 5 Click Select Private Link Label.

The Select Private Link Label window appears.

Step 6 Search for the appropriate private link label.

Search for the private link label that you created using the procedures provided in Tasks To Perform Prior to Configuring Service EPGs, on page 9.

Step 7 Click Add Selector.

Step 8 Enter a name in the Name field.

Step 9 Click the Key drop-down list to choose a key.

The options are:

- Choose Custom if you want to create a custom endpoint selector.
- Choose Region if you want to use the Azure region for the endpoint selector.
- Choose Cloud Resource Name if you want to use the service resource's name for the endpoint selector.

  For example, to select an SQL server with the name `ProdSqlServer`, you would choose Name in the Key field, and you would enter `ProdSqlServer` in the Value field later in these procedures.
- Choose Cloud Resource ID if you want to use the cloud provider's ID for the endpoint selector.

  For example, to select an SQL server using the cloud provider's resource ID, you would choose Resouce ID in the Key field, and you would enter the value of the selector, such as `/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer`, in the Value field later in these procedures.

Step 10 Click the Operator drop-down list to choose an operator.

The options are:

- equals: Used when you have a single value in the Value field.
- not equals: Used when you have a single value in the Value field.
- in: Used when you have multiple comma-separated values in the Value field.
- not in: Used when you have multiple comma-separated values in the Value field.
- has key: Used if the expression contains only a key.
- does not have key: Used if the expression contains only a key.

Step 11 Enter a value in the Value field then click the check mark to validate the entries.

The value you enter depends on the choices you made for the Key and Operator fields.

Step 12 When finished, click the check mark to validate the selector expression.

Step 13 Determine if you want to create additional expressions for the selector.

If you create more than one expression under a single selector, a logical AND exists between those expressions.

For example, assume you created two sets of expressions under a single selector:

- Selector 1, expression 1:
  - Key: Region
  - Operator: equals
  - Value: `westus`
- Selector 1, expression 2:
  - Key: Cloud Resource Name
  - Operator: equals
  - Value: `ProdSqlServer`

In this case, if both of these expressions are true (if the region is `westus` AND if the name attached to the resource is `ProdSqlServer`), then that endpoint is assigned to the service EPG.

Step 14 Click the check mark after every additional expression that you want to create under this selector, then click Add when finished.

Step 15 If you want to create additional endpoint selectors, click Add Endpoint Selector again and repeat these steps to create additional endpoint selectors.

If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you had created endpoint selector 1 as described in the previous step, and then you created a second endpoint selector as described below:

- Endpoint selector 2, expression 1:
  - Key: Region
  - Operator: in

- Value: `eastus`, `centralus`

In this case:

- If the region is `westus` AND the name attached to the resource is `ProdSqlServer` (endpoint selector 1 expressions)

  OR

- If the region is either `eastus` or `centralus` (endpoint selector 2 expression)

Then that end point is assigned to the service EPG.

Step 16 Click Save when finished.

Configuring Cloud Native Managed as the Deployment Type

Use the procedures in this section to configure Cloud Native Managed as the deployment type for the service EPG.

Procedure

Step 1 Navigate to site local.

Step 2 In the middle pane, scroll down to EPGs and click the service EPG that you just created.

Step 3 In the right pane, scroll down to the Selectors area.

Step 4 Click Add Selector.

The Add Selector window appears.

Step 5 In the Add Selector window, enter a name in the Name field.

Step 6 Click the Key drop-down list to choose a key.

At this time, IP is the only option available as a key for this access type.

Step 7 Click the Operator drop-down list to choose an operator.

The options are:

- equals: Used when you have a single value in the Value field.
- not equals: Used when you have a single value in the Value field.
- in: Used when you have multiple comma-separated values in the Value field.
- not in: Used when you have multiple comma-separated values in the Value field.
- has key: Used if the expression contains only a key.
- does not have key: Used if the expression contains only a key.

Step 8 Enter the appropriate IP address or a subnet in the Value field then click the check mark to validate the entries.

Enter the IP address or subnet that you created using the procedures provided in Tasks To Perform Prior to Configuring Service EPGs, on page 9.

Step 9 When finished, click the check mark to validate the selector expression.

Step 10 Determine if you want to create additional endpoint selector expressions to the endpoint selector.

If you create more than one expression under a single endpoint selector, a logical AND exists between those expressions.

For example, assume you created two sets of expressions under a single endpoint selector:

- Endpoint selector 1, expression 1:
  - Key: IP
  - Operator: equals
  - Value: 192.1.1.1/24
- Endpoint selector 1, expression 2:
  - Key: IP
  - Operator: not equals
  - Value: 192.1.1.2

In this case, if both of these expressions are true (if the IP address belongs to subnet 192.1.1.1/24 AND the IP address is not 192.1.1.2), then that endpoint is assigned to the service EPG.

Step 11 Click the check mark after every additional expression that you want to create under this endpoint selector, then click Add when finished.

You are returned to the Create EPG screen, with the new endpoint selector and the configured expressions shown.

Step 12 If you want to create additional endpoint selectors, click Add Endpoint Selector again and repeat these steps to create additional endpoint selectors.

If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you had created endpoint selector 1 as described in the previous step, and then you created a second endpoint selector as described below:

- Endpoint selector 2, expression 1:
  - Key: IP
  - Operator: equals
  - Value: 192.2.2.2/24

In this case:

- If the IP address belongs to subnet 192.1.1.1/24 AND the IP address is not 192.1.1.2 (endpoint selector 1 expressions)

  OR

- If the IP address belongs to subnet 192.2.2.2/24

Then that end point is assigned to the service EPG.

Step 13 Click Save when finished.

Configuring Third-Party as the Deployment Type

Use the procedures in this section to configure Third-Party as the deployment type for the service EPG. Private is the only option available to you as an access type. This means that you will use only private endpoints to the service, if the service offers it.

Note You must choose Custom as the Service Type if you choose Third-Party as the Deployment Type.

Procedure

Step 1 Navigate to site local.

Step 2 In the middle pane, scroll down to EPGs and click the service EPG that you just created.

Step 3 In the right pane, scroll down to the Selectors area.

The Select Private Link Label option becomes available with this access type. A private link label is used to associate the subnets to the service EPGs.

Step 4 Click Select Private Link Label.

The Select Private Link Label window appears.

Step 5 Search for the appropriate private link label.

Search for the private link label that you created using the procedures provided in Tasks To Perform Prior to Configuring Service EPGs, on page 9.

Step 6 Click Add Selector.

The Add Selector window appears.

Step 7 In the Add Endpoint Selector window, enter a name in the Name field.

Step 8 Click the Key drop-down list to choose a key.

At this time, URL is the only option available as a key for this access type, where you will use the alias or fully qualified domain name (FQDN) that identifies the service for the endpoint selector.

Step 9 Click the Operator drop-down list to choose an operator.

The options are:

- equals: Used when you have a single value in the Value field.
- not equals: Used when you have a single value in the Value field.
- in: Used when you have multiple comma-separated values in the Value field.
- not in: Used when you have multiple comma-separated values in the Value field.
- has key: Used if the expression contains only a key.
- does not have key: Used if the expression contains only a key.

Step 10 Enter a valid URL in the Value field then click the check mark to validate the entries.

Step 11 When finished, click the check mark to validate the selector expression, then click Add.

You are returned to the Create EPG screen, with the new endpoint selector and the configured expression shown.

Step 12 If you want to create additional endpoint selectors, click Add Endpoint Selector again and repeat these steps to create additional endpoint selectors.

If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors.

For example, assume you created two endpoint selectors as described below:

- Endpoint selector 1:
  - Key: URL
  - Operator: equals
  - Value: `www.acme1.com`
- Endpoint selector 2:
  - Key: URL
  - Operator: equals
  - Value: `www.acme2.com`

In this case:

- If the URL is `www.acme1.com`

  OR

- If the URL is `www.acme2.com`

Then that end point is assigned to the service EPG.

Step 13 Click Save when finished.

Trademarks

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.